

FILED  
IN CLERK'S OFFICE  
U.S. DISTRICT COURT E.D.N.Y.

CCC  
F.#2016R02148

★ FEB 28 2017 ★

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

LONG ISLAND OFFICE

-----X

IN THE MATTER OF THE SEARCH OF:

AFFIDAVIT IN  
SUPPORT OF A  
SEARCH WARRANT

THE PREMISES KNOWN AND  
DESCRIBED AS AN APPLE I-PHONE, MODEL  
6, WITH A WHITE FACE/ GOLD BACK WITH  
IMEI 354410065105960.

(T. 21, U.S.C., §§ 841(a)(1) and 846)

-----X

MJ - 17 0185

EASTERN DISTRICT OF NEW YORK, SS:

ROBERT T. STUEBER, being duly sworn, deposes and states that he is a  
Task Force Officer with the Drug Enforcement Administration ("DEA"), duly appointed  
according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is  
located in THE PREMISES KNOWN AND DESCRIBED AS AN APPLE I-PHONE  
CELLULAR TELEPHONE, MODEL 6, WITH A WHITE FACE/ GOLD BACK, IMEI  
354410065105960 (the "DEVICE") further described in Attachment A, the things described  
in Attachment B, which constitute evidence, fruits, and instrumentalities of conspiracy to  
distribute a controlled substance, in violation of Title 21, United States Code, Section 846,  
distribution of a controlled substance causing the death of Nicholas Weber, in violation of  
Title 21, United States Code, Section 841(b)(1)(C), and possessing with intent to distribute a  
controlled substance, in violation of Title 21, United States Code, Section 841(a)(1).

The source of your deponent's information and the grounds for his belief are as follows:<sup>1</sup>

1. I am a Task Force Officer with the DEA. I have been employed by the DEA for approximately five years and have been a detective with the Suffolk County Police Department ("SCPD") for approximately fifteen years. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for the unlawful possession, distribution, and manufacture of controlled substances. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from my own observations, reports made to me by other law enforcement officers, information obtained from confidential sources of information, and review of records from the DEA and other law enforcement agencies. In addition, when I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

#### BACKGROUND

3. On or about May 17, 2016, Nicholas Weber died from acute heroin intoxication at his residence in Kings Park, New York. Based on interviews of witnesses, examination of surveillance videos, and analysis of cellular telephone records, among other

---

<sup>1</sup> Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

things, the government's investigation revealed that RICHARD JACOBELLIS supplied the heroin that killed Weber. Specifically, on or about May 16, 2016, Weber contacted his friend ("CS 1") and asked CS 1 if CS 1 knew anyone who sold heroin.<sup>2</sup> CS 1 tried to discourage Weber from using heroin explaining that Weber could become addicted. Weber responded that he only used heroin occasionally and would never become addicted because of his busy schedule. CS 1 then contacted JACOBELLIS and asked whether he was willing to sell heroin to Weber. The next day, JACOBELLIS agreed to sell heroin to Weber.

4. On or about May 17, 2016, JACOBELLIS arrived at Weber's house in Kings Park shortly before 8 p.m. One of Weber's neighbors had a video camera that captured JACOBELLIS arriving at Weber's house in a dark-colored Volkswagen at that time. JACOBELLIS exited his dark-colored Volkswagen and entered Weber's basement. He encountered Weber and one of Weber's friends ("CS 2").<sup>3</sup> JACOBELLIS proceeded to sell \$100 worth of heroin to Weber. JACOBELLIS instructed Weber to erase his phone number and text messages. CS 2 witnessed this drug transaction and heard JACOBELLIS's instruction to erase the incriminating communications. JACOBELLIS left as did CS 2. CS 1 and CS 2 identified JACOBELLIS as the person on the neighbor's surveillance video and also confirmed that JACOBELLIS drove a dark-colored Volkswagen. Moreover, records

---

<sup>2</sup> CS 1 has proven to be reliable and credible as information by him/her has been corroborated by other sources, including, but not limited to, other witnesses, telephone records, cellular telephone forensic analysis, text messages, Facebook messages, DMV records and video/ audio recordings.

<sup>3</sup> CS 2 has proven to be reliable and credible as information by him/her has been corroborated by other sources, including, but not limited to, other witnesses, telephone records, cellular telephone forensic analysis, text messages, Facebook messages, DMV records and video/ audio recordings.



from the New York State Department of Motor Vehicles show that JACOBELLIS was driving a blue Volkswagen at the time of this drug transaction.

5. About 15 minutes later at 8:11 p.m., Weber sent a message to CS 1 inviting CS 1 to come to his house. A little after 8:30 p.m., CS 1 arrived at Weber's house and found Weber unresponsive in the basement. CS 1 got Weber's parents who administered CPR and called 911. They were unable to save Weber's life. An autopsy was performed that concluded that the cause of Weber's death was "Acute Heroin Intoxication."

6. The government's investigation determined that JACOBELLIS was using a computer application from a company called PINGER to communicate with Weber to set up the drug transaction that caused Weber's death--PINGER is a computer application that attempts to disguise the cellular telephone number of the user. Additionally, the investigation revealed that JACOBELLIS was using Facebook messenger to communicate regarding his drug business

7. On or about January 13, 2017, a confidential informant ("CI"), acting at the direction of law enforcement officers, contacted JACOBELLIS via Facebook messenger for the purpose of arranging a heroin transaction.<sup>4</sup> JACOBELLIS gave the CI his telephone number and agreed to sell heroin to the CI. Shortly thereafter, JACOBELLIS met the CI and consummated the transaction, which meeting was recorded using both audio and video equipment.

8. For this criminal conduct, on or about February 2, 2017, a grand jury sitting in the Eastern District of New York returned a three-count indictment charging

---

<sup>4</sup> CI has proven to be reliable and credible as information by him/her has been corroborated by other sources, including, but not limited to, other witnesses, telephone records, DMV records and video/ audio recordings.



JACOBELLIS with distributing heroin on May 17, 2016 that caused the death of Nick Weber (Count Two), conspiring to distribute heroin from May 2016 through January 2017 (Count One) and distributing heroin to the CI on January 13, 2017 (Count Three). See United States v. Jacobellis, 17-CR-052 (JS). On that same day, the Honorable Anne Shields, United States Magistrate Judge for the Eastern District of New York, signed a warrant authorizing JACOBELLIS's arrest. On or about February 7, 2107, JACOBELLIS was arrested and was in possession of the DEVICE.

9. Based on my training and experience and discussions with other law enforcement officers, I know that individuals involved in the distribution and possession with intent to distribute narcotics often do not act alone and often communicate with coconspirators by means of cellular telephones such as the DEVICE. They commonly maintain records that reflect names, addresses, or telephone numbers of their associates in their cellular telephones. They also commonly maintain records of communications such as call logs, chats and text messages in their cellular telephones. They also commonly take photographs of themselves, their associates, or their property using their cellular telephones. These individuals usually maintain these records of communication and photographs in their possession and in their cellular telephones.

10. Based on my knowledge, training, and experience, I know that the DEVICE can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the DEVICE. This information can sometimes be recovered with forensic tools.

11. Law enforcement officers seized the DEVICE. Since its seizure, the DEVICE has been in law enforcement custody. There is therefore probable cause to believe that the DEVICE contains evidence, fruits, and instrumentalities of federal crimes.

#### TECHNICAL TERMS

12. As used herein, the following terms have the following meanings:

a. Wireless telephone (or mobile or cellular telephone): A handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving and storing text messages and email; taking, sending, receiving and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device, and a wide variety of applications, also known as "apps," which may store the user's preferences and other data. Such apps may include Facebook, Twitter, and other social media services.

b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178).

Every computer or other electronic device, such as the DEVICE, that connects to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.

13. Based on my research, I know that the DEVICE provides not only phone and text message services, but can also be used to send and receive emails; access the Internet; track GPS data; take, store and share photographs and videos; and use a wide variety of apps. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the DEVICE.

#### TECHNICAL BACKGROUND

14. As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the DEVICE were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence can be recovered from the DEVICE because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and instant



messaging/“chat” programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use.

Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, instant messaging or chat logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device

is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding user attribution evidence, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

15. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.


16. Because this application seeks only permission to examine the DEVICE, which is already in law enforcement's possession, the execution of the warrant does not involve intrusion into a physical location. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

#### CONCLUSION

17. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that on the DEVICE there exists evidence of crimes. Accordingly, a search warrant is requested.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS AN APPLE I-PHONE CELLULAR TELEPHONE, MODEL 6, WITH A WHITE FACE/ GOLD BACK, IMEI 354410065105960.

Dated: Central Islip, New York  
February 28, 2017

  
\_\_\_\_\_  
Robert T. Stueber  
Task Force Officer, DEA

Sworn to before me this  
28<sup>th</sup> day of February, 2017

~~/s/ Steven Locke~~ STEVEN I. LOCKE  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK



ATTACHMENT A

Property To Be Searched

The property to be searched is THE PREMISES KNOWN AND DESCRIBED AS AN APPLE I-PHONE CELLULAR TELEPHONE, MODEL 6, WITH A WHITE FACE/ GOLD BACK, IMEI 354410065105960 (the "DEVICE"). The warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things To Be Seized

All information obtained from the DEVICE will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes fruits, evidence and instrumentalities of conspiracy to distribute controlled substance in violation of Title 21, United States Code, Section 846, distribution of a controlled substance causing death of Nicholas Weber, in violation of Title 21, United States Code, Section 841(b)(1)(C), and possessing with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 841(a)(1), including:

1. All records and information on the DEVICE described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of conspiracy to distribute controlled substance in violation of Title 21, United States Code, Section 846, distribution of a controlled substance causing death of Nicholas Weber, in violation of Title 21, United States Code, Section 841(b)(1)(C), and possessing with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 841(a)(1);

2. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;

7. Evidence of the times the DEVICE was used;

8. Passwords, encryption keys, and other access devices that may be necessary to access the DEVICE; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of conspiracy to distribute controlled substance, in violation of Title 21, United States Code, Section 846, distribution of a controlled substance causing death of Nicholas Weber, in violation of Title 21, United States Code, Section 841(b)(1)(C), and possessing with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 841(a)(1).

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been



created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.